

REMARKS

This responds to the Office Action mailed on February 23, 2004.

Applicant acknowledges and appreciates the phone conference between Applicant's representative, Joseph P. Mehrle, and the Examiner conducted April 21, 2004. During that conference, Applicant's representative discussed the viability of the one of the references. No further discussions or subject matter related to the claims or the invention and Final Office Action were discussed.

Claims 1-20 are presently pending in the application.

§103 Rejection of the Claims

Claims 1-20 were rejected under 35 USC § 103(a) as being unpatentable over Mashayekhi et al.(U.S. 5,818,936) in view of Viavant et al.(U.S. 5,784,566). It is of course fundamental that in order to sustain an obviousness rejection and ever step or element of the rejected claims must be taught or suggested in the combination of cited references.

Applicant has reviewed the Examiner's newly stated reasons for rejection and continues to respectfully disagree. The Examiner asserts that the "private key" taught by Mashayekhi is the same as the "common key" recited in Applicant's independent claims. However, one of ordinary skill in the art would not agree with this interpretation because a private key is never exchanged (not even in encrypted format) in a public/private key relationship; rather, the each party maintains their own unique private key.

Moreover, with a public-private key pair the public key is never negotiated between the parties; rather the public keys are unilaterally and uniquely established by each of the parties. Additionally, each party needs the other party's public key to successfully decrypt a piece of data. Thus, a public key is not a common key either because there are two separate public keys, which are entirely different from one another and both unique public keys are needed by a single party in a relationship along with that party's unique private key to successfully decrypt a single piece of data. *Emphasis added.*

In fact the terms "common" and "private" on their faces are opposites of one another. Common connotes mutual knowledge to more than one participant, whereas private connotes

unilateral knowledge by only one participant. In traditional Public Key Infrastructure (PKI) architectures, private keys are never expressed as common and private keys are not generally disclosed or transmitted beyond a machine that natively houses the private key. Therefore, on this point, Applicant disagrees with the Examiner in that claim interpretation cannot be based on meanings that running contrary to the references and contrary to how terms are generally understood in the art. Applicant cannot craft any correct and fair interpretation of the phrase “common key” which would include traditional public-private keys in traditional PKI technology.

Additionally, Applicant would like to point out that the independent claims of the present invention teach specific multi-layered types of encryption that require an authentication secret to be encrypted with a common key; that common key is further encrypted with a session key. Applicant cannot find any teaching in Viavant that supports the Examiner’s contention that this portion of the Applicant’s independent claims is disclosed or suggested by Viavant.

That is, the authentication secret cannot be obtained until the common key is known, since the authentication secret is encrypted with the common key. The common key is encrypted with the session key. Thus, in order to acquire the authentication secret a client needs to decrypt the common key and then decrypt the authentication secret (two layers and types of encryption). These positively recited claim limitations clearly require multiple levels of encryption, using different keys in order to acquire a single item of data (authentication secret); and this is not taught, disclosed, or suggested in the Viavant reference as the Examiner has concluded.

More specifically, in Viavant a single encryption service is used and there is not dual encryption on a single piece of data (authentication secret). Applicant’s dual encryption of a single piece of data using different keys (common and session) is novel and is not taught or suggested in the Viavant reference, in the Mashayekhi reference, or in the combination of the two cited references.

Applicant’s unique arrangement provides a new and novel protection for authentication secrets distributed over a network, because, traditionally, which is consistent with what is described and taught in the Viavant patent; data is simply encrypted with a single key. Conversely, Applicant has used two distinct keys (common and session) to dual encrypt a single piece of data (authentication secret). This adds a new and novel dimension to traditional security

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.116 – EXPEDITED PROCEDURE

Serial Number: 09/518664

Filing Date: March 3, 2000

Title: APPARATUS AND METHOD FOR AUTOMATICALLY AUTHENTICATING A NETWORK CLIENT

Page 4

Dkt: 1565.027US1

approaches by decoupling the session key from yet another encryption key (common key) and thereby providing additional security over the network wire for distribution of the authentication secret.

Thus, Applicant respectfully requests that the present rejection be reconsidered and that the Examiner withdraw the rejections and allows the present independent claims.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (513) 942-0224 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

CAMERON MASHAYEKHI

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.

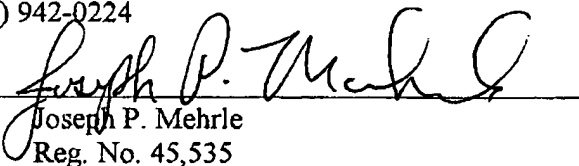
P.O. Box 2938

Minneapolis, MN 55402

(513) 942-0224

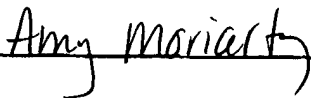
Date 4-23-04

By


Joseph P. Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 23rd day of April, 2004.

Name



Signature

